

#2
PATENTS

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of

Makiba SHIGEZUMI

Serial No. (unknown)

Filed herewith

DNS SERVER FILTER



CLAIM FOR FOREIGN PRIORITY UNDER 35 U.S.C. 119
AND SUBMISSION OF PRIORITY DOCUMENT

Assistant Commissioner for Patents

Washington, D.C. 20231

Sir:

Attached hereto is a certified copy of applicant's corresponding patent application filed in Japan on January 21, 2000, under No. 12757/2000.

Applicant herewith claims the benefit of the priority filing date of the above-identified application for the above-entitled U.S. application under the provisions of 35 U.S.C. 119.

Respectfully submitted,

YOUNG & THOMPSON

By

Benoît Castel

Benoît Castel
Attorney for Applicant
Customer No. 000466
Registration No. 35,041
745 South 23rd Street
Arlington, VA 22202
Telephone: 703/521-2297

January 2, 2001

日 本 国 特 許 庁

PATENT OFFICE
JAPANESE GOVERNMENT

1c914 U.S. PRO
09/750914
01/02/01

別紙添付の書類に記載されている事項は下記の出願書類に記載されて
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed
with this Office.

出 願 年 月 日
Date of Application:

2000年 1月21日

出 願 番 号
Application Number:

特願2000-012757

出 願 人
Applicant (s):

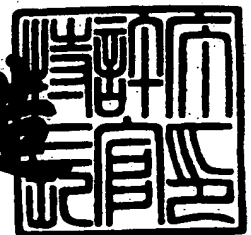
日本電気株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

2000年 9月22日

特許庁長官
Commissioner,
Patent Office

及川耕造



【書類名】 特許願

【整理番号】 65000524

【提出日】 平成12年 1月21日

【あて先】 特許庁長官 殿

【国際特許分類】 H04L 12/66
G06F 13/00
H04L 12/46

【発明者】

【住所又は居所】 東京都港区芝五丁目 7 番 1 号 日本電気株式会社内

【氏名】 重住 牧

【特許出願人】

【識別番号】 000004237

【氏名又は名称】 日本電気株式会社

【代理人】

【識別番号】 100080816

【弁理士】

【氏名又は名称】 加藤 朝道

【電話番号】 045-476-1131

【手数料の表示】

【予納台帳番号】 030362

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9304371

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 DNSサーバフィルタ

【特許請求の範囲】

【請求項1】

受信したDNS (Domain Name System) パケットについて、該パケットをDNSサーバに渡すまえに、該パケットの内容に異常があるか否か検査するパケット検証手段を備え、異常を検出した際にエラー応答パケットを生成して要求元に返す、ことを特徴とするDNSサーバフィルタ装置。

【請求項2】

組織外の者が組織外のネットワークから送信するホスト名、ドメイン名、IP (Internet Protocol) アドレスに関する情報をDNSプロトコルを通じて取得するためのDNSパケットを前記パケット検証手段で検査し、異常があればエラー応答を返し、組織外の者が組織のネットワーク構成情報を利用して組織のネットワークに侵入を行うこと、及び、異常な形式のパケットを受信することでDNSサーバが動作異常になること、を未然に防ぐようした、ことを特徴とする請求項1記載のDNSサーバフィルタ装置。

【請求項3】

組織内の端末から組織外のネットワークに属するDNSサーバに送信するホスト名、ドメイン名、IPアドレスに関する情報をDNSプロトコルを通じて取得するためのDNSパケットを、前記パケット検証手段で検査し、異常があればエラー応答を返し、組織外のネットワークに属するDNSサーバを動作異常とさせることを未然に防ぐようにした、ことを特徴とする請求項1記載のDNSサーバフィルタ装置。

【請求項4】

前記パケット検証手段によるパケットの異常検出の条件について、追加、及び削除自在とされている、ことを特徴とする請求項1乃至3のいずれか一に記載のDNSサーバフィルタ装置。

【請求項5】

請求項1乃至4のいずれか一に記載の前記DNSサーバフィルタ装置を、ファ

イアウォール装置内に実装し、

前記ファイアウォール装置の前記DNSサーバフィルタ装置は、前記ファイアウォール装置が設置される組織の管理外の第1のネットワークと、組織内の第2のネットワークとをセキュリティを保ちながら相互接続し、DNSについて、前記第1のネットワークに属する端末が前記第2のネットワークに属する端末のホスト名とIPアドレスの情報やネットワークの名前空間に関する情報を取得すること、

前記第1のネットワークに属する端末から前記第1のネットワークを通じてDNSサーバに対してDNSプロトコル上不正なパケットを送付してDNSサーバに動作異常を引き起こすこと、

前記第2のネットワークに属する端末やDNSサーバが前記第1のネットワークに属する端末や前記第1のネットワークに属するホストに対してDNSプロトコル上異常なパケットを送付すること、

を防ぐようにした、ことを特徴とするファイアウォール装置。

【請求項6】

パケットフィルタリング型のファイアウォール装置と、

ファイアウォール装置と通信接続する請求項1乃至4のいずれかーに記載の前記DNSパケットフィルタ装置と、

前記DNSパケットフィルタ装置と通信接続するDNSサーバと、を備えたことを特徴とするネットワークシステム。

【請求項7】

DNSプロトコルにおける端末及びDNSサーバからの問い合わせ、及び、DNSサーバからの応答パケットを受信するパケット受信部と、

問い合わせ要求を管理するためのセッション管理テーブルを備え、問い合わせ及び応答パケットを管理し全体の制御を行うセッション管理部と、

問い合わせ及び応答パケットが異常であるか否かを検査するパケット検証部と、

DNSサーバへの問い合わせパケットを生成する要求生成部と、

問い合わせパケットの送信元に返す応答パケットを生成する応答生成部と、

問い合わせ及び応答パケットを送信するパケット送信部と、
 を備え、受信したDNSプロトコルのパケットについて該パケットをDNSサーバに渡すまえに、内容に異常があるか否か検査し、異常を検出した際に、エラー応答パケット生成して要求元に返す、ことを特徴とするDNSサーバフィルタ装置。

【請求項 8】

前記パケット検証部が、
 検証プログラムのエントリポイントアドレス情報と、検証プログラムの実行の優先順位情報と、検証プログラムの属性情報とを備えたプログラム管理テーブルを備え、前記検証プログラムの属性を参照し、実行すべき検証プログラムを選択して実行に移す制御を行う呼出管理部と、
 検証プログラムを格納した記憶装置と、
 管理ツールもしくは設定ファイルで指示された検証プログラムの実行ファイルをメモリ上にロードし、ロードされた検証プログラムを初期化し、検証プログラムのエントリポイントを、入手した属性と共に、前記呼出管理部のプログラム管理テーブルに登録し、前記管理ツールで削除が指示された検証プログラムをメモリ上から解放処理を行うように制御するロード管理部と、
 実行される検証プログラムから呼び出されるDNSサーバフィルタ本体の機能を利用するためのサブルーチン群よりなるサービスルーチンと、
 を備えている、ことを特徴とする請求項 7 記載のDNSサーバフィルタ装置。

【請求項 9】

前記セッション管理テーブルが、要求パケットへのポインタと、問い合わせ要求を行った要求元のIPアドレスと、問い合わせ要求を行った要求元ポート番号と、問い合わせ要求のパケット形式が正常であった場合に問い合わせ要求を別のDNSサーバに転送しているかどうかを示すフラグと、を備え、
 前記パケット受信部が、DNSパケットを受信すると、該パケットを前記セッション管理部に渡し、
 前記セッション管理部は、前記セッション管理テーブルに、受信したパケットの送信元のIPアドレス、受信したパケットのポート番号を設定し、テスト中を意味

する値をフラグを設定したのち、受信パケットを、前記パケット検証部に渡してパケットの検査を依頼し、

前記パケット検証部で前記受信パケットの検査を行った結果、検査結果に問題がある場合、前記セッション管理部が、前記受信パケットの種別を調べて、問い合わせ要求であるか否か判定し、問い合わせ要求であれば、前記セッション管理部は、前記応答生成部に対して、エラー応答パケットの生成を依頼し、

生成されたパケットを、前記セッション管理テーブルの要求元IPアドレス、ポート番号で指定される相手に対して、前記パケット送信部に送信を依頼し、受信したパケットについて、前記セッション管理テーブルに登録されている情報を削除して、受信した問い合わせ要求パケットを解放し、

受信パケットが問い合わせ要求でない場合には、前記セッション管理部は、前記セッション管理テーブルを検索して、元の問い合わせ要求に関する部分を取り出し、検索された前記セッション管理テーブルのエントリの要求パケットへのポインタから、問い合わせ要求パケットを参照して、これを基に、前記応答生成部に対して、エラー応答パケットの生成を依頼し、前記セッション管理テーブルの要求元IPアドレス、及びポート番号で指定される相手に対して、生成した応答パケットを送信するように、前記パケット送信部に対して依頼し、受信した応答パケットについて、前記セッション管理テーブルに登録されている情報を削除して応答パケットを解放するとともに、該応答パケットに対応する問い合わせ要求について、前記セッション管理テーブルに登録されているエントリも削除する、ことを特徴とする請求項8記載のDNSサーバフィルタ装置。

【請求項10】

前記パケット検証部でパケットの検査を行い、検査結果に問題がない場合、前記セッション管理部が受信パケットの種別を調べ、応答パケットの場合、前記セッション管理部は、該応答パケットに対応する問い合わせ要求の情報を、前記セッション管理テーブルから検索し、前記セッション管理部が受信した応答パケットが元の問い合わせ要求に対する回答となっているかどうかを調べ、

前記調査の結果、さらに問い合わせを行う必要があれば、前記セッション管理部は、受信した応答パケットの情報から次の問い合わせ先を決定して、前記要求生

成部に問い合わせ要求パケットの生成を依頼し、前記パケット送信部に対して次の問い合わせ先への送信を依頼し、

前記セッション管理部は、受信した問い合わせの途中経過である応答パケットに関する情報を、前記セッション管理テーブルから削除して応答パケットを解放し、

前記調査の結果、元々の問い合わせパケットに対する回答となる応答パケットを受信した場合には、前記セッション管理部は、応答パケットを受信した応答パケットの結果を反映させた元の問い合わせ要求に対する応答パケットの生成を前記応答生成部に依頼し、前記パケット送信部に元の問い合わせ要求の送信元に対して送信を依頼し、受信した応答パケットに関連する情報を前記セッション管理テーブルから削除し、元の問い合わせ要求に関する情報を前記セッション管理テーブルから削除し応答パケットを解放する、ことを特徴とする請求項 9 記載の DNS サーバフィルタ装置。

【請求項 1 1】

前記パケット検証部でパケットの検査を行い、検査結果に問題がない場合、前記セッション管理部が受信パケットの種別を調べ、受信したパケットが問い合わせ要求である場合、前記セッション管理部が受信パケットの送信元を調べ、前記送信元が組織内部のネットワークからの問い合わせでない場合、組織外のネットワークの問い合わせ要求を解決するために前記セッション管理部は、まず最初に問い合わせる組織外の DNS サーバを決定し、元の問い合わせ要求を元にした問い合わせ要求の生成を前記要求生成部に依頼し、その問い合わせ要求パケットを、前記決定された DNS サーバに対して送信するようにパケット送信部に依頼し、

前記送信元が組織内部のネットワークからの問い合わせである場合、前記セッション管理部は受信した問い合わせ要求パケットを元に要求生成部に問い合わせ要求パケットの生成を依頼し、DNS サーバに対する問い合わせパケットの送信を前記パケット送信部に依頼し、

前記セッション管理部は、受信したパケットに対応する前記セッション管理テーブルのエントリ中のフラグに、「問い合わせ中」の値を設定し、受信パケットへのポインタを前記セッション管理テーブルのエントリのポインタに設定する、ことを特徴とする請求項 9 又は 1 0 記載の DNS サーバフィルタ装置。

【請求項12】

DNSサーバ情報をあらかじめ蓄えておくキャッシュメモリを備えたことを特徴とする請求項7記載のDNSサーバフィルタ装置。

【請求項13】

(a) DNSプロトコルにおける端末及びDNSサーバからの問い合わせ、及びDNSサーバからの応答パケットを通信装置を介して受信するパケット受信処理と、

(b) 問い合わせ要求を管理するためのセッション管理テーブルを備え、問い合わせ及び応答パケットを管理し全体の制御を行うセッション管理処理と、

(c) 問い合わせ及び応答パケットが異常であるか否かを検査するパケット検証処理と、

(d) DNSサーバへの問い合わせパケットを生成する要求生成処理と、

問い合わせパケットの送信元に返す応答パケットを生成する応答生成処理と、

(e) 問い合わせ及び応答パケットを通信装置を介して送信するように制御するパケット送信処理と、

を備え、受信したDNSパケットについて該パケットをDNSサーバに渡すまえに、内容に異常があるか否か検査し、異常を検出した際に、エラー応答パケット生成して返すという、DNSサーバフィルタの処理を、コンピュータ上で実行させるためのプログラムを記録した記録媒体。

【請求項14】

請求項13記載の記録媒体において、検証プログラムのエントリポイントアドレス情報と、検証プログラムの実行の優先順位情報と、検証プログラムの属性情報とを備えたプログラム管理テーブルを備え、

前記パケット検証処理が、前記検証ソフトウェアの属性を参照し、実行すべき検証プログラムを選択して実行に移す制御を行う呼出管理処理と、

管理ツールもしくは設定ファイルで指示された検証プログラムの実行ファイルをメモリ上にロードし、ロードされた検証プログラムを初期化し、検証プログラムのエントリポイントを入手した属性と共に前記プログラム管理テーブルに登録し、及び前記管理ツールで削除を指示された検証プログラムのメモリ上からの解

放処理を行うロード管理処理と、

検証プログラムから呼び出されるDNSサーバフィルタ本体の機能を利用するためのサブルーチン群よりなるサービスルーチン処理と、

の各処理を、前記コンピュータ上で実行させるためのプログラムを記録した記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、ネットワークシステムに関し、特に、IPアドレスとドメイン名との対応の管理を行うドメインネームシステム（DNS）のフィルタ装置に関する。

【0002】

【従来の技術】

DNS (Domain Name System) は、インターネット等のTCP/IP (Transport Control Protocol/Internet Protocol) を用いたプロトコル（トランスポート層としてUDP (User Datagram Protocol) も含む）によるネットワークにおいて接続されたホストの名前とIPアドレスとを関連付けた情報等をTCP/IPネットワークに接続されたホストに提供する、TCP/IPプロトコル上のサービスである。DNSでは、ホストが属している組織に対してドメイン名と呼ばれる名前でもとめられており、ドメイン名は、国家レベル、企業、学術組織等の組織の種別毎、組織名毎、組織内の部署毎に階層的に名付けられ、ホスト名はドメイン名と組み合わせることで、TCP/IPネットワークにおける唯一性が保証される。例えば、インターネットに接続された日本の企業の日本電気株式会社のWWW (World Wide Web) サーバは、日本を示す“jp”、企業を示す“co”、日本電気株式会社を示す“nec”、同社において名付けられたWWWサーバのホスト名を示す“www”を、“www.nec.co.jp”という記述方法で表現される。

【0003】

“www.nec.co.jp”の“nec.co.jp”はインターネット

におけるドメイン名割り当て機関であるNIC (Network Information Center) により割り当てられた日本電気株式会社を示すドメイン名であり、“www”は日本電気株式会社内で割り当てられたホスト名である。TCP/IPプロトコルで通信しようとするホストは、接続先のホストのIPアドレスを知らなければならず、このWWWサーバにTCP/IPで接続しようとするインターネットに接続されたホストは、“www.nec.co.jp”という名前に対応するIPアドレスをDNSサーバに問い合わせる。“www.nec.co.jp”に接続しようとするホストは、まずルートサーバと呼ばれるDNSにおけるドメイン階層構造の頂点の情報を管理するDNSサーバに問い合わせ、“jp”ドメインを管理しているDNSサーバを教えてもらい、次にその“jp”ドメインを管理しているDNSサーバに問い合わせ、“co.jp”ドメインを管理しているDNSサーバを教えてもらい、次に“co.jp”ドメインを管理しているDNSサーバに問い合わせ、“nec.co.jp”を管理しているDNSサーバを教えてもらい、次に“nec.co.jp”ドメインを管理しているDNSサーバに“www.nec.co.jp”というホスト名に対するIPアドレスを問い合わせ、そのDNSサーバにその名前があればこのホストのIPアドレスを返す。

【0004】

インターネットに接続する組織において、セキュリティ上の理由により、インターネットに接続する部分にファイアウォールを設置して、直接、TCP/IPプロトコルによる組織外との通信を制限する場合がある。

【0005】

組織のセキュリティ要件として、組織外秘の情報の保護の為に組織外からのTCP/IPプロトコルを通じた組織内資源へのアクセスを制限することが挙げられる。

【0006】

DNSにおいても、組織内のネットワークに接続されたホストの名前やIPアドレスについての情報やその組織の部署名やネットワーク構成が名付けられているドメイン名をできる限り隠すことによって、侵入者がこの情報を用いて、組織

内のネットワークに侵入することを防ぐことが要請されている。

【0007】

【発明が解決しようとする課題】

上記要請に対して、従来のシステムでは、組織内のDNSサーバとは別にファイアウォールの外に設置された組織外のホストからのアクセスを許可するホストに関する情報を提供するDNSサーバを設置し、組織内のDNSサーバは、組織内のホストが組織外のホストのDNS情報を取得するためにファイアウォールの外に設置されたDNSサーバに対して、再帰的に問い合わせできるように設定し、ファイアウォールの外に設置されたDNSサーバから、組織内のDNSサーバに対しては、問い合わせができないように、DNSサーバ及びファイアウォールに設定することで対処している。

【0008】

かかる構成の従来のシステムにおいては、DNSサーバを複数台設置することや、DNSサーバの管理が複雑化する、といった問題点が生じている。

【0009】

また、セキュリティ上の問題としては、不正な形式のパケットを攻撃対象のサーバに送信する事で、バグ等のサーバプログラムの実装上の問題によりサービスが停止させる「DoS (Denial of Service) アタック」と呼ばれる攻撃に対しても防御が必要となり、DNSサービスについても指摘されている。

【0010】

従来、このような問題が指摘されると、サービスプログラムの開発者が、サービスプログラムを修正する必要があった。

【0011】

たしかに、一部のサービスプログラムは、そのプログラムのソースファイルが公開されているため (UNIXTM用 bind 等)、サービスプログラムの利用者がソースに対する修正差分を入手するか、利用者が修正を行ってコンパイルすることで、サービスプログラムをDoSアタックに対応するものに交換することが可能とされている。

【 0 0 1 2 】

しかしながら、ソースファイルが公開されていない場合（例えばMicrosoft社製Windows NT Server 4.0に含まれるDNSサーバ等の場合）、サービスプログラム開発者が修正モジュールをサービスプログラム利用者に配布するまでに時間を要し、DOSアタック等の問題が指摘されてから長い間、この問題に対して、適切な対処を施すことができない状態にあった。

【 0 0 1 3 】

またソースファイルが公開されていても、利用者自身のプログラミングスキルの不足等の理由により、適切に対処できない場合もある。

【 0 0 1 4 】

以上、DOSアタックについて説明したが、サービスは停止しないにしても、サービスプログラムの実装上の問題により、本来得られるべき正常な応答が返らない場合も、同様の問題が発生する。

【 0 0 1 5 】

また、組織のネットワークセキュリティ管理上、組織内部から組織外のホストに対してセキュリティ上脅威となる攻撃を行うことが可能とならないように、対策を施さなければならないといったセキュリティ要件を掲げる組織も存在する。

【 0 0 1 6 】

なお、米国特許第5,805,820号には、DNSにおいて、ドメインの内部情報に対する問い合わせ要求をリダイレクト（redirect）することで、組織内ネットワークのドメイン名及びIPアドレス等のネットワーク構成情報（private information）をDNSを通じて組織外に送信しないようにした方法及びこれを実現する装置について提案されているが、DOSアタック等の問題には対処できていない。

【 0 0 1 7 】

したがって本発明は、上記問題点に鑑みてなされたものであって、その目的は、組織外の者が組織のネットワーク構成情報を利用して組織のネットワークに侵入を行う事を防ぐとともに、異常な形式のパケットを受信する事でDNSサーバの動作が異常になる事を未然に防ぐ、DNSサーバフィルタ及び記録媒体を提供

することにある。

【0018】

【課題を解決するための手段】

前記目的を達成する本発明のDNSサーバフィルタは、受信したDNSパケットについて、該パケットをDNSサーバに渡すまえに、該パケットに異常があるか否か検査するパケット検証手段を備え、異常を検出した際に、エラー応答パケット生成して、要求元に返す、構成とされている。

【0019】

本発明は、DNSプロトコルにおける端末及びDNSサーバからの問い合わせ、及びDNSサーバからの応答パケットを受信するパケット受信部と、問い合わせ要求を管理するためのセッション管理テーブルを備え、問い合わせ及び応答パケットを管理し全体の制御を行うセッション管理部と、問い合わせ及び応答パケットが異常であるか否かを検査するパケット検証部と、DNSサーバへの問い合わせパケットを生成する要求生成部と、問い合わせパケットの送信元に返す応答パケットを生成する応答生成部と、問い合わせ及び応答パケットを送信するパケット送信部と、を備え、受信したDNSパケットについて該パケットをDNSサーバに渡すまえに、内容に異常があるか否か検査し、異常を検出した際に、エラー応答パケット生成して要求元に返す。

【0020】

【発明の実施の形態】

本発明の実施の形態について説明する。本発明のDNS (Domain Name System) サーバフィルタは、RFC (Request For Comments) 1034、1035、及びこれに関連するRFC文書により定義されたDNSプロトコルによりIPアドレスとホスト名及びドメイン名の対応に関連付けるサービスを行うDNSサーバを含むネットワークシステムにおいて、DNSパケットを、DNSサーバに渡す前に、その内容を検査し、異常があれば、エラー応答を返し、検査のための処理を、利用者が追加及び削除する事を可能としている。

【0021】

本発明によれば、

- ・ 外部ネットワークからの異常な形式のDNSパケットを受信することによりDNSサーバが異常動作を引き起こすこと、
- ・ 内部ネットワークのホストが異常な形式のDNSパケットをDNSサーバが外部ネットワークに送信することで外部ネットワークに属するホストを異常動作させること、
- ・ 組織外の侵入者が内部ネットワークの情報を得るために外部ネットワークからアクセスして内部ネットワークの名前情報を取得すること、等のセキュリティ上の攻撃から、内部ネットワークのDNSサーバと内部ネットワークシステムを防御し、外部ネットワークに対してDNSプロトコルを通じて異常な動作を引き起こさせたり、セキュリティ上の攻撃を行うことを防ぎ、DNSに関する問題の素早い対応を可能としている。

【 0 0 2 2 】

本発明は、DNSプロトコルにおける端末及びDNSサーバからの問い合わせ、及びDNSサーバからの応答パケットを受信するパケット受信部（2）と、DNS問い合わせ要求を管理するためのセッション管理テーブル（8）を備え、問い合わせ及び応答パケットを管理し全体の制御を行うセッション管理部（3）と、問い合わせ及び応答パケットが異常であるか否かを検査するパケット検証部（4）と、DNSサーバへの問い合わせパケットを生成する要求生成部（5）と、問い合わせパケットの送信元に返す応答パケットを生成する応答生成部（6）と、問い合わせ及び応答パケットを送信するパケット送信部（7）と、を備え、受信したDNSパケットについて該パケットをDNSサーバに渡す前に、内容に異常があるか否かを検査し、異常を検出した際に、エラー応答パケット生成して要求元へ返す。

【 0 0 2 3 】

パケット検証部（4）が、検証プログラムのエントリポイントアドレスと、検証プログラムの実行の優先順位と、検証プログラムの属性情報とを備えたプログラム管理テーブル（40）を備え、前記検証ソフトウェアの属性を参照し、実行すべき検証プログラムを選択して実行に移す制御を行う呼出管理部（30）と、

管理ツールもしくは設定ファイルで指示された検証プログラムの実行ファイルをメモリ上にロードし、ロードされた検証プログラムを初期化し、検証プログラムのエントリポイントを入手した属性と共に前記呼出管理部のプログラム管理テーブルに登録し、及び前記管理ツールで削除を指示された検証プログラムのメモリ上からの解放処理を行うロード管理部（36）と、検証プログラムから呼び出されるDNSサーバフィルタ本体の機能を利用するためのサブルーチン群よりなるサービスルーチン（31）と、を備えている。

【0024】

本発明は、その好ましい一実施の形態において、セッション管理テーブル（8）が、要求パケットへのポインタ（60）と、問い合わせ要求を行った要求元のIPアドレス（61）と、問い合わせ要求を行った要求元ポート番号（62）と、問い合わせ要求のパケット形式が正常であった場合に問い合わせ要求を別のDNSサーバに転送しているかどうかを示すフラグと（63）、を備え、パケット受信部（2）がDNSパケットを受信すると、該パケットを前記セッション管理部（3）に渡し、セッション管理部（3）は、セッション管理テーブル（8）に、受信したパケットの送信元のIPアドレス、受信したパケットのポート番号を設定し、テスト中を意味する値をフラグを設定したのち、セッション管理部（3）は、受信パケットをパケット検証部（4）に渡してパケットの検査を依頼し、パケット検証部（4）でパケットの検査を行い、検査結果に問題がある場合、前記セッション管理部（3）が受信パケットの種別を調べ、それが問い合わせ要求であるか否か判定し、問い合わせ要求であれば、前記セッション管理部は、前記応答生成部（6）に対して、エラー応答パケットの生成を依頼し、生成されたパケットを前記セッション管理テーブル（8）の要求元IPアドレス、ポート番号で指定される相手に対して、パケット送信部（7）に送信を依頼し、受信した応答パケットについて、セッション管理テーブル（8）に登録された情報を削除し、受信した問い合わせ要求パケットを解放する。

【0025】

また受信パケットが問い合わせ要求でない場合、セッション管理部（3）が、セッション管理テーブル（8）を検索して、元の問い合わせ要求に関する部分を取り

出し、検索されたセッション管理テーブル（８）のエントリの要求パケットへのポインタから、問い合わせ要求パケットを参照して、これを基に、応答生成部（６）に対して、エラー応答パケットの生成を依頼し、セッション管理テーブル（８）の要求元ＩＰアドレス、及びポート番号で指定される相手に対して、生成した応答パケットを送信するように、パケット送信部（７）に対して依頼し、受信した応答パケットについて、セッション管理テーブル（８）に登録されている情報を削除して応答パケットを解放するとともに、該応答パケットに対応する問い合わせ要求について、セッション管理テーブルに登録されているエントリも削除する。

【００２６】

またパケット検証部（４）でパケットの検査を行い、検査結果に問題がない場合、セッション管理部（３）が受信パケットの種別を調べ、応答パケットの場合、セッション管理部（３）は該応答パケットに対応する問い合わせ要求の情報を、前記セッション管理テーブル（８）から検索し、セッション管理部（３）が受信した応答パケットが元の問い合わせ要求に対する回答となっているかどうかを調べ、調査の結果、さらに問い合わせを行う必要があれば、セッション管理部（３）は、受信した応答パケットの情報から次の問い合わせ先を決定し、セッション管理部（３）は、要求生成部（５）に問い合わせ要求パケットの生成を依頼し、前記パケット送信部（７）に対して次の問い合わせ先への送信を依頼し、セッション管理部（３）は、受信した問い合わせの途中経過である応答パケットに関する情報を前記セッション管理テーブルから削除し応答パケットを解放し、前記調査の結果、元々の問い合わせパケットに対する回答となる応答パケットを受信した場合、セッション管理部（３）は、応答パケットを受信した応答パケットの結果を反映させた元の問い合わせ要求に対する応答パケットの生成を前記応答生成部（６）に依頼し、パケット送信部（７）に元の問い合わせ要求の送信元に対して送信を依頼し、受信した応答パケットに関連する情報をセッション管理テーブル（８）から削除し、元の問い合わせ要求に関する情報を前記セッション管理テーブル（８）から削除し応答パケットを解放する。

【００２７】

受信したパケットが問い合わせ要求である場合、セッション管理部（３）が受信

パケットの送信元を調べ、前記送信元が組織内部のネットワークからの問い合わせでない場合、組織外のネットワークの問い合わせ要求を解決するために前記セッション管理部は、まず最初に問い合わせる組織外のDNSサーバを決定し、元の問い合わせ要求を元にした問い合わせ要求の生成を要求生成部（５）に依頼し、その問い合わせ要求パケットを、前記決定されたDNSサーバに対して送信するようにパケット送信部に対して依頼し、前記送信元が組織内部のネットワークからの問い合わせである場合、セッション管理部（３）は受信した問い合わせ要求パケットを元に要求生成部（５）に問い合わせ要求パケットの生成を依頼し、DNSサーバに対する問い合わせパケットの送信をパケット送信部（７）に依頼し、セッション管理部（３）は、受信したパケットに対応するセッション管理テーブル（８）のエントリ中のフラグに、「問い合わせ中」の値を設定し、受信パケットへのポインタをセッション管理テーブル（８）のエントリのポインタに設定する。

【 0 0 2 8 】

本発明においては、（a）DNSプロトコルにおける端末及びDNSサーバからの問い合わせ、及びDNSサーバからの応答パケットを通信装置を介して受信するパケット受信処理と、

（b）DNS問い合わせ要求を管理するためのセッション管理テーブルを備え、問い合わせ及び応答パケットを管理し全体の制御を行うセッション管理処理と、

（c）問い合わせ及び応答パケットが異常であるか否かを検査するパケット検証処理と、

（d）DNSサーバへの問い合わせパケットを生成する要求生成処理と、

問い合わせパケットの送信元に返す応答パケットを生成する応答生成処理と、

（e）問い合わせ及び応答パケットを通信装置を介して送信するように制御するパケット送信処理と、

を備え、受信したDNSパケットについて該パケットをDNSサーバに渡すまえに、内容に異常があるか否かを検査し、異常を検出した際に、エラー応答パケット生成して返す、DNSサーバフィルタの前記各処理は、コンピュータ上で実行プログラムを実行することで実現される。この場合、該プログラムを記録した記録媒体からプログラムを読み出し装置を介して、もしくは通信媒体を介してダウ

ンロードしてコンピュータに読み出しインストールし該プログラムの実行形式をコンピュータの主メモリにロードして実行することで、本発明のDNSサーバフィルタを実施することができる。

【0029】

【実施例】

本発明の実施例について図面を参照して以下に説明する。図1は、本発明の一実施例のDNSサーバフィルタの構成を示す図である。図1を参照すると、DNSサーバフィルタ1は、DNSプロトコルにおける端末及びDNSサーバからの問い合わせ及びDNSサーバからの応答パケットを受信するパケット受信部2と、問い合わせ及び応答パケットを管理し全体の制御を行うセッション管理部3と、問い合わせ及び応答パケットが異常であるか否かを検査するパケット検証部4と、DNSサーバへの問い合わせパケットを生成する要求生成部5と、問い合わせパケットの送信元に返す応答パケットを生成する応答生成部6と、問い合わせ及び応答パケットを送信するパケット送信部7と、を備えて構成されている。またセッション管理部3は、DNS問い合わせ要求を管理するためのセッション管理テーブル8を持つ。

【0030】

図2は、本発明の一実施例のDNSサーバフィルタ1をファイアウォール内に実装した場合の構成の一例を示す図である。図2において、ファイアウォール10は、インターネットの様な、これが置かれる組織の管理外のネットワーク15と、組織内のネットワーク16とを、セキュリティを保ちながら相互接続する役割を持ち、DNSについて、

- ・ネットワーク15に属する端末17がネットワーク16に属する端末18のホスト名とIPアドレスの情報やネットワーク16の名前空間に関する情報を取得すること、

- ・端末17からネットワーク15を通じてDNSサーバ11に対してDNSプロトコル上不正なパケットを送付することで、DNSサーバ11に動作異常を引き起こすこと、

- ・端末18やDNSサーバ11が端末17やネットワーク15に属するホスト

に対してDNSプロトコル上異常なパケットを送付すること、

を防ぐ機能を具備することが要請されており、本発明の一実施例においては、DNSサーバフィルタ1により、これらの機能要件を満たしている。

【0031】

DNSサーバ11は、NIC (Network Interface Card) 13が属するサブネットワーク等のネットワーク15のDNS情報の一部と、ネットワーク16のDNS情報の一部を管理し、DNSプロトコルに従い問い合わせに対する応答する機能を持つ。

【0032】

TCP/IPドライバ12は、NIC13及びNIC14を通じて、TCP/IPプロトコルで通信を行うための制御を行うものであり、DNSサーバフィルタ1やDNSサーバ11はこのTCP/IPドライバ12上で動作するプロセスである。

【0033】

また、ファイアウォール10は、端末17から直接TCP/IPプロトコルにより端末18と通信を行うことを許可しない設定（一般的にこの様な設定をIP forward (フォワード) がoff (オフ) であるという) となっており、DNSサーバフィルタ1はNIC13、DNSサーバ11はNIC14のIPアドレス宛に送付された問い合わせ要求のみ受け付けるように設定されている。

【0034】

図3は、本発明の一実施例のDNSサーバフィルタ1を1台の装置に実装し、組織のネットワークに設置した場合の構成を示す図である。図3において、ファイアウォール20は、パケットフィルタリング型ファイアウォールであり、図2のファイアウォールとは異なり、組織外ネットワーク15に属する端末17と組織のネットワーク16に属する端末18間での直接のTCP/IPプロトコルによる通信を、ファイアウォール20の設定により、許可されたポートやアドレスに限り可能としている。

【0035】

図3において、ファイアウォール20は、ネットワーク16を保護する目的で

設置され、DNSプロトコルについてみると、端末17がネットワーク15を経由してDNSプロトコルでアクセスできるのは、DNSサーバフィルタ1のみであり、組織内のDNSサーバ11にはアクセスが許可されておらず、また、DNSサーバ11や端末18も、直接DNSプロトコルでネットワーク15上のホストへのアクセスは許可されていない設定とされている。

【0036】

組織のネットワーク16に属するファイアウォール20、DNSサーバフィルタ1、DNSサーバ11、端末18の間は、DNSプロトコルに限らず、任意のTCP/IP上のプロトコルで通信可能である。

【0037】

DNSサーバ11は、DNSサーバフィルタ1に対してフォワードの設定を行っている。即ち、DNSサーバ11に対して、端末18からのネットワーク15に属する端末17のドメイン名やIPアドレスの問い合わせ要求を受信すると、DNSサーバ11は、該問い合わせ要求が、ネットワーク16に属さないホストに関するものであると認識し、該問い合わせ要求を、DNSサーバフィルタ1に転送（フォワード）する。また端末18が参照するDNSサーバは、DNSサーバ11に設定されている。

【0038】

図4は、本発明の一実施例のDNSサーバフィルタ1におけるパケット検証部4の構成を示す図である。図4を参照すると、呼出管理部30は、検証プログラム（ソフトウェア）32、33、34、35の属性を参照して実行すべきものを選択して実行に移す制御を行うものであり、検証プログラムを管理するためのプログラム管理テーブル40を備えている。

【0039】

ロード管理部36は、

・管理端末を備え操作指示情報を入力する管理ツール38、もしくは設定ファイル39の情報で指示された検証プログラムの実行ファイル37を不図示のメモリ（DNSサーバフィルタが実装されるコンピュータのメモリ）上にロードする処理、

- ・メモリ上にロードされた検証プログラムの初期化処理を実行させ、
 - ・検証プログラムのエントリポイントを手した属性と共に呼出管理部 3 0 が持つプログラム管理テーブル 4 0 に登録する処理、
 - ・管理ツール 3 8 で削除を指示された検証プログラムのメモリ上からの解放処理、
- を行う。

【 0 0 4 0 】

サービスルーチン 3 1 は、検証プログラム 3 2、3 3、3 4、3 5 の開発を容易にするための検証プログラムから呼び出される DNS サーバフィルタ本体の機能を使うためのサブルーチン群である。

【 0 0 4 1 】

図 7 は、図 4 のプログラム管理テーブル 4 0 のエントリの一例である。テーブルの各エントリは、

- ・検証プログラムのエントリポイントアドレス 5 0 と、
- ・検証プログラムにより指定される実行の優先順位 5 1 と、
- ・検証プログラムにより指定される検証プログラムの属性 5 2 と、を備えて構成されている。

【 0 0 4 2 】

図 8 は、本発明の一実施例の DNS サーバフィルタにおけるセッション管理テーブル 8 のエントリの一例である。テーブルの各エントリは、

- ・要求パケットへのポインタ 6 0 と、
- ・問い合わせ要求を行った要求元 IP アドレス 6 1 と、
- ・問い合わせ要求を行った要求元ポート番号 6 2 と、
- ・問い合わせ要求のパケット形式が正常であった場合に問い合わせ要求を別の DNS サーバに転送しているかどうかを示すフラグ 6 3 と、を備えている。

【 0 0 4 3 】

図 5 及び図 6 は、DNS サーバフィルタ 1 の動作処理を説明するためのフローチャートである。図 9 は、図 4 のパケット検証部 4 の検証プログラムの実行のフローチャートである。

【 0 0 4 4 】

本発明の一実施例のDNSサーバフィルタ1の動作について以下に説明する。

【 0 0 4 5 】

まず、図1、図5乃至図8を参照して、DNSサーバフィルタ1の動作について説明する。

【 0 0 4 6 】

ステップS101において、DNSパケットを、パケット受信部2が受信すると、そのパケットをセッション管理部3に渡し、ステップS102では、セッション管理部3は、管理テーブル8にその受信したパケットの送信元のIPアドレスを項目61（図8参照）に、受信したパケットのポート番号を項目62に入れ、フラグ63に「テスト中」を意味する値を設定する。

【 0 0 4 7 】

次のステップS103において、セッション管理部3は、受信パケットを、パケット検証部4に渡してパケットの検査を依頼し、パケット検証部4でパケットの検査を行う。

【 0 0 4 8 】

ステップS104において、パケット検証部4による検査結果に問題があるか否か判定し、正常終了すれば（問題がない場合）、ステップS111に進み、異常終了すれば、ステップS105に進む。

【 0 0 4 9 】

ステップS105では、セッション管理部3が受信パケットの種別を調べ、それが問い合わせ要求（DNS要求）か否か判定し、DNS要求であれば、ステップS106、応答パケットであればステップS108に進む。

【 0 0 5 0 】

ステップS106では、この情報の問い合わせ元に対してエラー応答を返さなければならない状態であるため、セッション管理部3は、応答生成部6に対して、エラー応答パケットの生成を依頼し、生成されたパケットを、管理テーブル8の項目61、62の相手に対して、パケット送信部7に送信を依頼する。

【 0 0 5 1 】

次のステップ S 1 0 7 では、受信した応答パケットについて、管理テーブル 8 に登録された情報を削除し、受信した問い合わせ要求パケットを解放して終了する。

【 0 0 5 2 】

一方、ステップ S 1 0 5 において、受信パケットが DNS 要求でなく、ステップ S 1 0 8 に移行するという状態は、以前、この DNS サーバフィルタ 1 に対して正常な問い合わせ要求が送られ、別の DNS サーバに対して問い合わせ要求を行っている状態であるが、その結果が異常であったため、元々の問い合わせ要求を行ったホストに対して、問い合わせが失敗したことを示すエラー応答を返さなければならないことを意味している。このため、ステップ S 1 0 8 では、セッション管理部 3 が、セッション管理テーブル 8 を検索して、元の問い合わせ要求に関する部分を取り出す。

【 0 0 5 3 】

次のステップ S 1 0 9 では、検索された管理テーブル 8 のエントリの項目 6 0 から、問い合わせ要求パケットを参照して、これを基に、応答生成部 6 に対して、エラー応答パケットの生成を依頼し、管理テーブル 8 の項目 6 1、6 2 の相手に対して、生成した応答パケットを送信するように、パケット送信部 7 に対して依頼する。

【 0 0 5 4 】

次のステップ S 1 1 0 では、受信した応答パケットについて、管理テーブル 8 に登録されている情報を削除し、応答パケットを解放し、また、これに対応する問い合わせ要求について、管理テーブル 8 に登録されているエントリも削除して、終了する。

【 0 0 5 5 】

ステップ S 1 0 4 の判定の結果、検査結果正常であった場合には、図 6 のステップ S 1 1 1 に分岐する。

【 0 0 5 6 】

図 6 のステップ S 1 1 1 において、セッション管理部 3 が受信パケットの種別を調べ、それが問い合わせ要求パケットであれば、ステップ S 1 1 9 に進み、応答

パケットであればステップ S 1 1 2 に進む。

【 0 0 5 7 】

ステップ S 1 1 2 では、セッション管理部 3 が、この応答パケットに対応する問い合わせ要求の情報を、管理テーブル 8 から検索する。

【 0 0 5 8 】

次のステップ S 1 1 3 では、セッション管理部 3 が受信した応答パケットが元の問い合わせ要求に対する回答となっているかどうかを調べる。

【 0 0 5 9 】

元々の問い合わせ要求に、DNS プロトコルにおける再帰問い合わせが指定されていない場合には、そのまま応答パケットとほぼ同じ形の応答パケットを返せば良いが、再帰問い合わせが指定されている場合には、DNS サーバフィルタ 1 が回答を得るまで DNS サーバに対して問い合わせを行う必要がある。例えば、“www. foo. co. jp” というホスト名に対する IP アドレスを検索する場合には、

- ・ ルート DNS サーバ、
- ・ “jp” ドメインを管理している DNS サーバ、
- ・ “co. jp” ドメインを管理している DNS サーバ、
- ・ “foo. co. jp” ドメインを管理している DNS サーバ、

を順に問い合わせることになり、その途中の DNS サーバからは次の DNS サーバのアドレスしか教えてもらえない（例えば“co. jp” ドメインの DNS サーバからは“foo. co. jp” ドメインを管理している DNS サーバのアドレスについて教えてもらえない）ため、元々の問い合わせ要求に対しては、この応答パケットは問い合わせ途中の状況を示すに過ぎず、回答にはなり得ない。

【 0 0 6 0 】

ステップ S 1 1 3 において、このような調査を行い、さらに問い合わせを行う必要があれば、ステップ S 1 1 4 に、必要がなければステップ S 1 1 7 に進む。

【 0 0 6 1 】

ステップ S 1 1 4 の状態は、DNS サーバフィルタ 1 で、さらに他の DNS サーバに対して問い合わせが必要であることを意味している。このため、ステップ

S114において、セッション管理部3は、受信した応答パケットの情報から次の問い合わせ先を決定する。

【0062】

そして、次のステップS115では、セッション管理部3が問い合わせ要求パケットを要求生成部5に問い合わせ要求パケットの生成を依頼し、次の問い合わせ先にパケット送信部7に送信を依頼する。

【0063】

次のステップS116では、セッション管理部3は、受信した問い合わせの途中経過である応答パケットに関する情報を管理テーブル8から削除し、応答パケットを解放して終了する。

【0064】

ステップS117の状態は、元々の問い合わせパケットに対する回答となる応答パケットを受信したことを意味している。このため、ステップS117では、セッション管理部3は、応答パケットを受信した応答パケットの結果を反映させた元の問い合わせ要求に対する応答パケットの生成を応答生成部6に依頼し、パケット送信部7に元の問い合わせ要求の送信元に対して送信を依頼する。

【0065】

次のステップS118では、受信した応答パケットに関連する情報を管理テーブル8から削除し、元の問い合わせ要求に関する情報を管理テーブル8から削除し、応答パケットを解放して終了する。

【0066】

ステップS111の判定の結果、受信したパケットが問い合わせ要求（DNS要求）である場合、ステップS119において、セッション管理部3が受信パケットの送信元を調べ、それが組織内部のネットワークからの問い合わせであればステップS122に進み、そうでなければステップS120に進む。

【0067】

ステップS120の状態は、組織外のネットワークの問い合わせ要求を解決するために、DNSサーバフィルタ1が問い合わせ元に代わって組織外のDNSサーバに対して問い合わせを開始しなければならないことを意味している。このた

め、ステップS120では、セッション管理部3は、まず最初に問い合わせる組織外のDNSサーバを決定する（多くの場合これは通常ルートサーバである）。

【0068】

次のステップS121では、セッション管理部3は、元の問い合わせ要求を元にした問い合わせ要求の生成を要求生成部5に依頼し、その問い合わせ要求パケットをステップS120で決定したDNSサーバに対して送信することをパケット送信部7に依頼する。

【0069】

一方、ステップS122の状態は、組織内部のネットワークに関する問い合わせを受けたことを意味する。組織内部のネットワークに関する情報を得るためには、DNSサーバフィルタ1は、組織内部のDNSサーバ11に問い合わせを転送（フォワード）する様になっている。

【0070】

このため、ステップS122では、セッション管理部3は受信した問い合わせ要求パケットを元に要求生成部5に問い合わせ要求パケットの生成を依頼し、DNSサーバ11に問い合わせパケットをパケット送信部7に送信を依頼する。

【0071】

ステップS123の状態は、問い合わせ要求を受信して現在DNSサーバフィルタ1が別のDNSサーバに問い合わせを行っていることを意味している。このため、ステップS123では、セッション管理部3は、受信したパケットに対応する管理テーブル8のエントリ中のフラグ63に、「問い合わせ中」の値を入れ、受信パケットへのポインタを管理テーブル8のエントリ中の項目60に入れて終了する。

【0072】

次に、図9を参照して、パケット検証部4について説明する。

【0073】

ステップS201では、パケット検証部4の呼出管理部30が持つ管理テーブル40を検索して、管理テーブル40中の優先順位51が最も大きい値のエントリを探し（実装では、各エントリは優先順位順に並んでいることが望ましい）、

エントリを確定する。

【0074】

次のステップS202では、未参照のエントリがあるかどうかを調べ、未参照のエントリが存在する場合、ステップS203に進む。

【0075】

ステップ203では、呼出管理部30が、管理テーブル40のエントリ中の属性52を調べて、対応する検証プログラムを実行すべきか否かを判断する。

【0076】

属性52は、各検証プログラムにより指定され、DNSサーバフィルタ1の初期化時に、設定ファイル38により、もしくは、実行中に、管理ツール38により、ロード管理部36による検証プログラムファイル37のロード後の検証プログラムの初期化処理時にロード管理部36に渡る値をロード管理部36が設定するものであり、問い合わせ要求パケットのチェックを行うもの、応答パケットのチェックを行うものといった検証プログラムの種類を示す値である。

【0077】

次のステップS204では、管理テーブル40の当該エントリに対応する検証プログラムを呼出管理部30が実行することに決定した場合、ステップS205に、そうでない場合はステップS207に進む。

【0078】

ステップS205では、呼出管理部30は、管理テーブル40の項目50にある検証プログラムのエントリポイントを呼び出す。

【0079】

ステップS206において、呼出管理部30は、ステップS205で呼び出した検証プログラムの結果を見て、正常終了か否か判定し、正常終了した場合ステップS207に進み、異常終了した場合、検証プログラムでエラーが発生した、すなわち受信したDNSのパケットは組織のセキュリティ要件に合致しない等の理由により受け付けられないと判断されたことになるため、エラーをパケット検証部4の呼出元であるセッション管理部3に渡して終了する。

【0080】

ステップ S 2 0 7 では、次の検証プログラムによる受信パケットのチェックを行うため、呼出管理部 3 0 は、先に行った検証プログラムの次に優先順位が高いもしくは同じ優先順位である検証プログラムを、管理テーブル 4 0 の優先順位 5 1 を参照して検索を行い、ステップ S 2 0 2 に進む。

【 0 0 8 1 】

この様にして、パケット検証部 4 は、ステップ S 2 0 2 からステップ S 2 0 7 を繰り返し、ステップ S 2 0 2 において、これ以上実行する検証プログラムが存在しないと判断された場合、これまで実行された全ての検証プログラムが正常終了したことを意味しており、受信した D N S パケットは組織のセキュリティ要件を満たしたものであることから、パケット検証部 4 は正常終了する。

【 0 0 8 2 】

次に、具体例に即して説明する。

【 0 0 8 3 】

図 2 は、D N S サーバフィルタ 1 をファイアウォール 1 0 内に実装した場合の構成を示す図である。組織外のネットワーク 1 5 に属する端末 1 7 が、組織内のネットワーク 1 6 に属する端末 1 8 の I P アドレスを取得しようと試みたとする。端末 1 7 は端末 1 8 のホスト名は知っているがその情報が格納されている D N S サーバは知らないものとする。

【 0 0 8 4 】

まず端末 1 8 は、組織外ネットワーク 1 5 に属する D N S サーバから組織のドメインを管理している D N S サーバの情報を入手し、その I P アドレスがファイアウォール 1 0 の N I C 1 3 に対応する I P アドレスであることが判明する。

【 0 0 8 5 】

次に端末 1 7 は、組織の D N S サーバと思っているファイアウォール 1 0 の N I C 1 3 の I P アドレス上で待ち合わせている D N S サーバフィルタ 1 に接続し、端末 1 8 のホスト名に対応する I P アドレスを問い合わせる。

【 0 0 8 6 】

問い合わせ要求を受けた D N S サーバフィルタ 1 は、パケット検証部 4 を呼び出して、この D N S パケットが組織のセキュリティ要件を満たすかどうかを検査

する。

【 0 0 8 7 】

もし、端末 1 7 が送信した DNS パケットの形式が異常であり、検証プログラムとして、これを検査するものが含まれていれば、そのパケットに対して検証プログラムはエラーを返し、DNS サーバフィルタ 1 は、端末 1 7 に対してエラー応答を返す。

【 0 0 8 8 】

もし端末 1 7 が送信した DNS パケットの形式が正常であるが、検証プログラムに、組織内部のホストに関する情報は提供しないことをセキュリティ要件を実現するためのプログラムが登録されている場合には、そのパケットに対して、検証プログラムはエラーを返し、DNS サーバフィルタ 1 は端末 1 7 に対してエラー応答を返す。

【 0 0 8 9 】

もし端末 1 7 が送信した DNS パケットの形式が正常であるが、検証プログラムに組織内部のホストに関する情報は提供しないことをセキュリティ要件を実現するためのプログラムが登録されていない場合には、DNS サーバフィルタ 1 は DNS サーバ 1 1 に要求を転送して端末 1 8 の IP アドレスを取得して応答として端末 1 7 に返す。

【 0 0 9 0 】

次に、図 2 に示した構成において、端末 1 8 が端末 1 7 の IP アドレスを入手する場合について説明する。

【 0 0 9 1 】

まず端末 1 8 は、組織内ネットワーク 1 6 の DNS サーバに組織外ネットワークの情報を要求するため、その DNS サーバはその問い合わせをファイアウォール 1 0 の NIC 1 4 で待ち合わせている DNS サーバ 1 1 に転送する。

【 0 0 9 2 】

DNS サーバ 1 1 は、組織外ネットワークについての問い合わせは DNS サーバフィルタ 1 1 に転送する様に設定されている。

【 0 0 9 3 】

問い合わせ要求パケットを受け取ったDNSサーバフィルタ1は、そのDNSパケットが正常であることを確認すると、組織外のDNSサーバに問い合わせ、応答パケットを得て、そのパケットが正常であれば、DNSサーバ11を通じて端末18に結果が返される。

【0094】

もし端末17のDNSサーバが異常な応答パケットを返してきた場合には、DNSサーバフィルタ1はDNSサーバ11にエラー応答を返し、端末18にもそのエラー応答が返る。

【0095】

異常な応答パケットとしては、例えば、形式が異常である他に、組織外との通信を盗聴する等の目的でDNSパケットの付加情報に偽の情報が書き加えられているといった事例が報告されている。

【0096】

図3は、DNSサーバフィルタ1が独立して組織内ネットワーク16に設置された例である。

【0097】

図3に示す構成において、DNSパケットのやりとりは、上述した図2に示すものとほぼ同じである。図2に示す構成では、端末17が直接DNSサーバ11にアクセスすることがTCP/IPドライバ12で禁じられているのに対し、図3に示す構成では、パケットフィルタ型ファイアウォール20により、禁止の設定が行われる点が相違している。

【0098】

本発明においては、パケット検証部4にあらかじめ登録しておいたドメインに属するホストに対する問い合わせがあった場合には、否定応答をを返すように判断する処理を実装することで、WWWサーバにおける「コンテンツフィルタリング」と呼ばれる技術の様な、組織の業務に無関係なホストへのアクセスを禁止するという要件を満たすためのシステムを構築することができる。

【0099】

また、本発明においては、DNSサーバフィルタに、DNSサーバ情報をあら

はじめ蓄えておくキャッシュメモリを追加することで、余分な問い合わせを減らすことができる。

【0100】

前記実施例では、本発明を説明するために、セキュリティに関連する処理を例に説明したが、本発明は、セキュリティに関連する目的にのみに限定されるものでないことは勿論である。

【0101】

【発明の効果】

以上説明したように、本発明によれば、組織外の者が組織外のネットワークから送信するホスト名、ドメイン名、IPアドレス等の情報をDNSプロトコルを通じて取得するためのDNSパケットを検査し、異常があればエラー応答を返す構成としたことにより、

- ・組織外の者が組織のネットワーク構成情報を利用して組織のネットワークに侵入を行うこと、及び、
 - ・異常な形式のパケットを受信する事でDNSサーバの動作が異常になること、を未然に防ぐことができる、
- という効果を奏する。

【0102】

また本発明によれば、組織内の者が組織外のネットワークに属するDNSサーバに送信するホスト名、ドメイン名、IPアドレス等の情報をDNSプロトコルを通じて取得するためのDNSパケットを検査し、異常があればエラー応答を返す構成としたことにより、組織外のネットワークに属するDNSサーバの動作を異常にさせる事未然に防ぐ事が可能となり、組織外のネットワークに属する他組織に対する組織の管理責任を果たすことができる、という効果を奏する。

【0103】

本発明のDNSサーバフィルタのパケット検証手段において、利用者による追加及び削除を可能とし、検証プログラムの記述方法を明示して、利用者自身で検証プログラムの作成を可能としたことにより、新たに判明したDNSサーバの問題に利用者による素早い対処を可能とし、またDNSサーバ自体を問題に対応さ

れたものに置換する場合は、問題に対応する不要な検証プログラムを削除してDNSサーバフィルタの性能を向上させることができる、という効果を奏する。

【図面の簡単な説明】

【図 1】

本発明の一実施例のDNSサーバフィルタの構成を示す図である。

【図 2】

本発明の一実施例のDNSサーバフィルタをファイアウォール内に実装した場合の構成を示す図である。

【図 3】

本発明の一実施例のDNSサーバフィルタを1台の装置に実装し、組織のネットワークに設置した場合の構成を示す図である。

【図 4】

本発明の一実施例におけるパケット検証部の構成を示す図である。

【図 5】

本発明の一実施例におけるDNSサーバフィルタの処理を説明するためのフローチャートである。

【図 6】

本発明の一実施例におけるDNSサーバフィルタの処理を説明するためのフローチャートである。

【図 7】

本発明の一実施例におけるパケット検証部のプログラム管理テーブルのエントリの一例を示す図である。

【図 8】

本発明の一実施例におけるセッション管理テーブルのエントリの一例を示す図である。

【図 9】

本発明の一実施例におけるパケット検証部の検証プログラムの処理手順を示すフローチャートである。

【符号の説明】

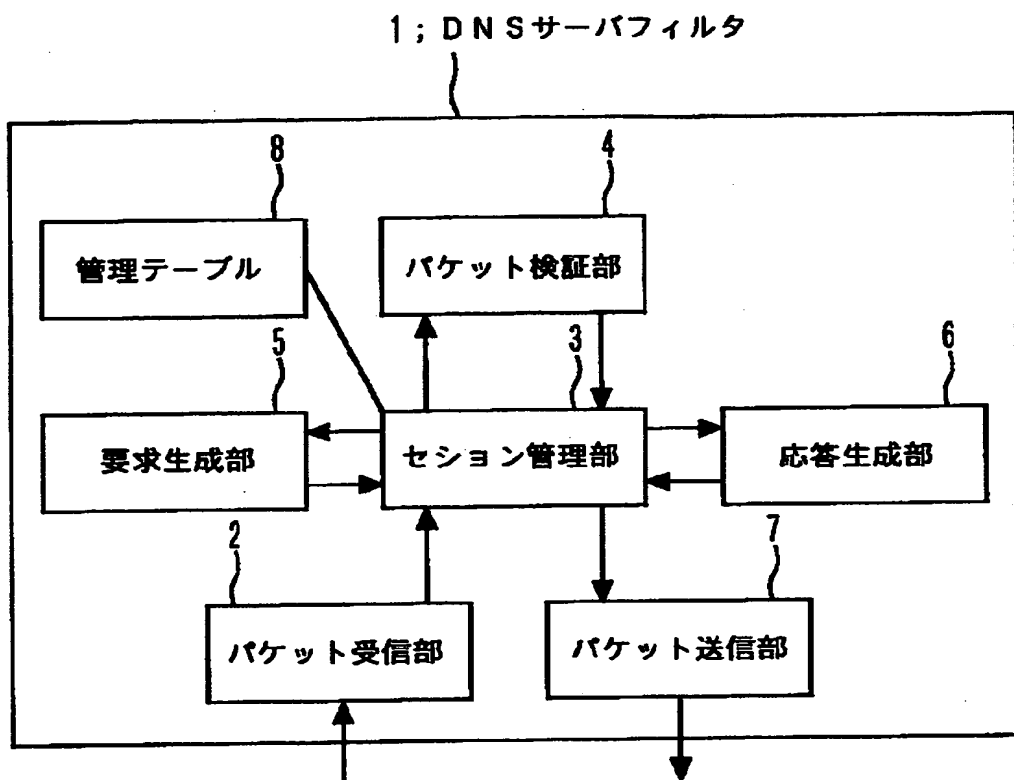
- 1 DNSサーバフィルタ
- 2 パケット受信部
- 3 セッション管理部
- 4 パケット検証部
- 5 要求生成部
- 6 応答生成部
- 7 パケット送信部
- 8 管理テーブル（セッション管理テーブル）
- 10 ファイアウォール
- 11 DNSサーバ
- 12 TCP/IPドライバ
- 13、14 NIC
- 15、16 ネットワーク
- 17、18 端末
- 20 ファイアウォール
- 30 呼出管理部
- 31 サービスルーチン
- 32～35 検証プログラム
- 36 ロード管理部
- 37 検証プログラム
- 38 管理ツール
- 39 設定ファイル
- 40 管理テーブル（検証プログラム管理テーブル）
- 50 エントリポイントアドレス
- 51 優先順位
- 52 属性
- 60 要求パケットへのポインタ
- 61 要求元IPアドレス
- 62 要求元ポート番号

63 フラグ

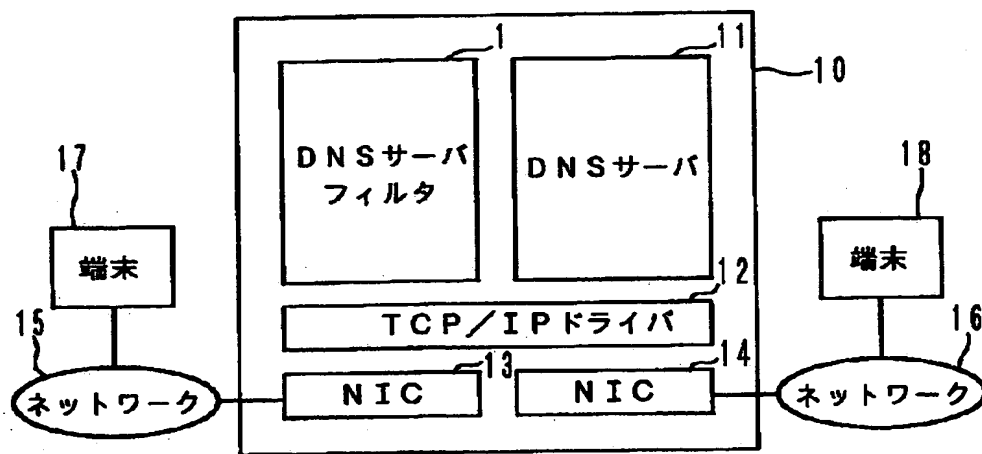
【書類名】

図面

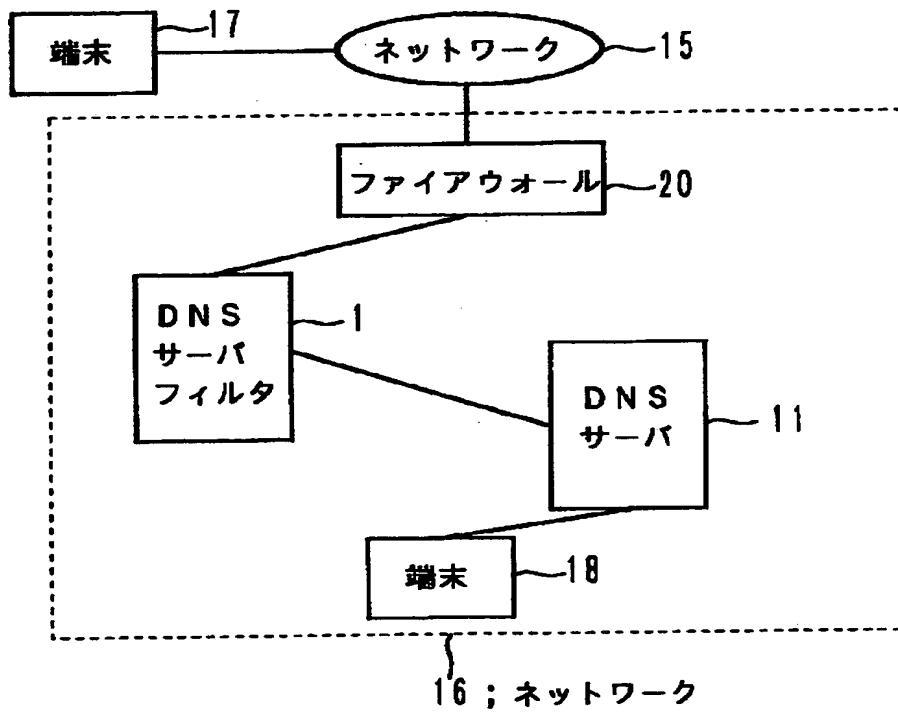
【図1】



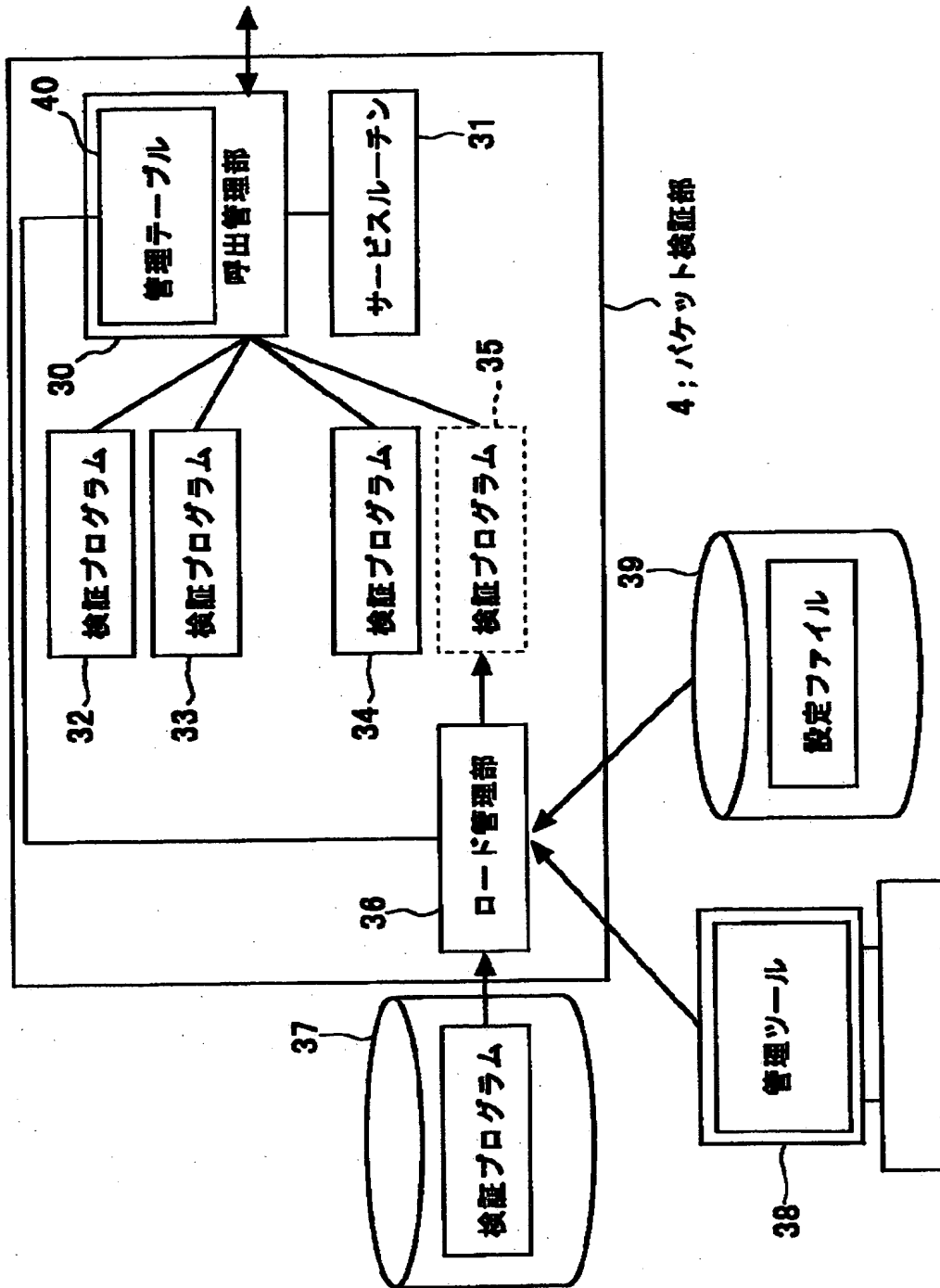
【図2】



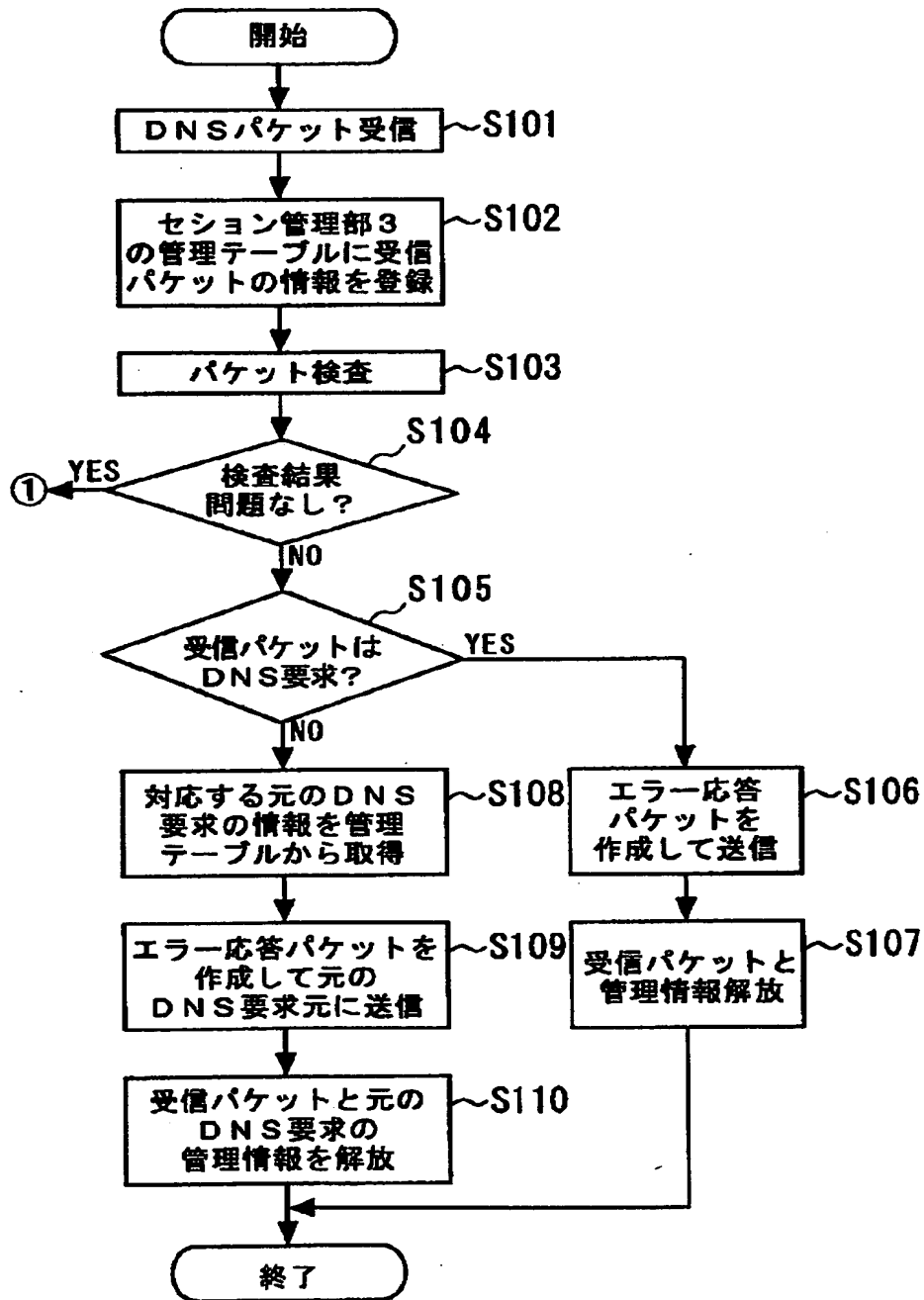
【図3】



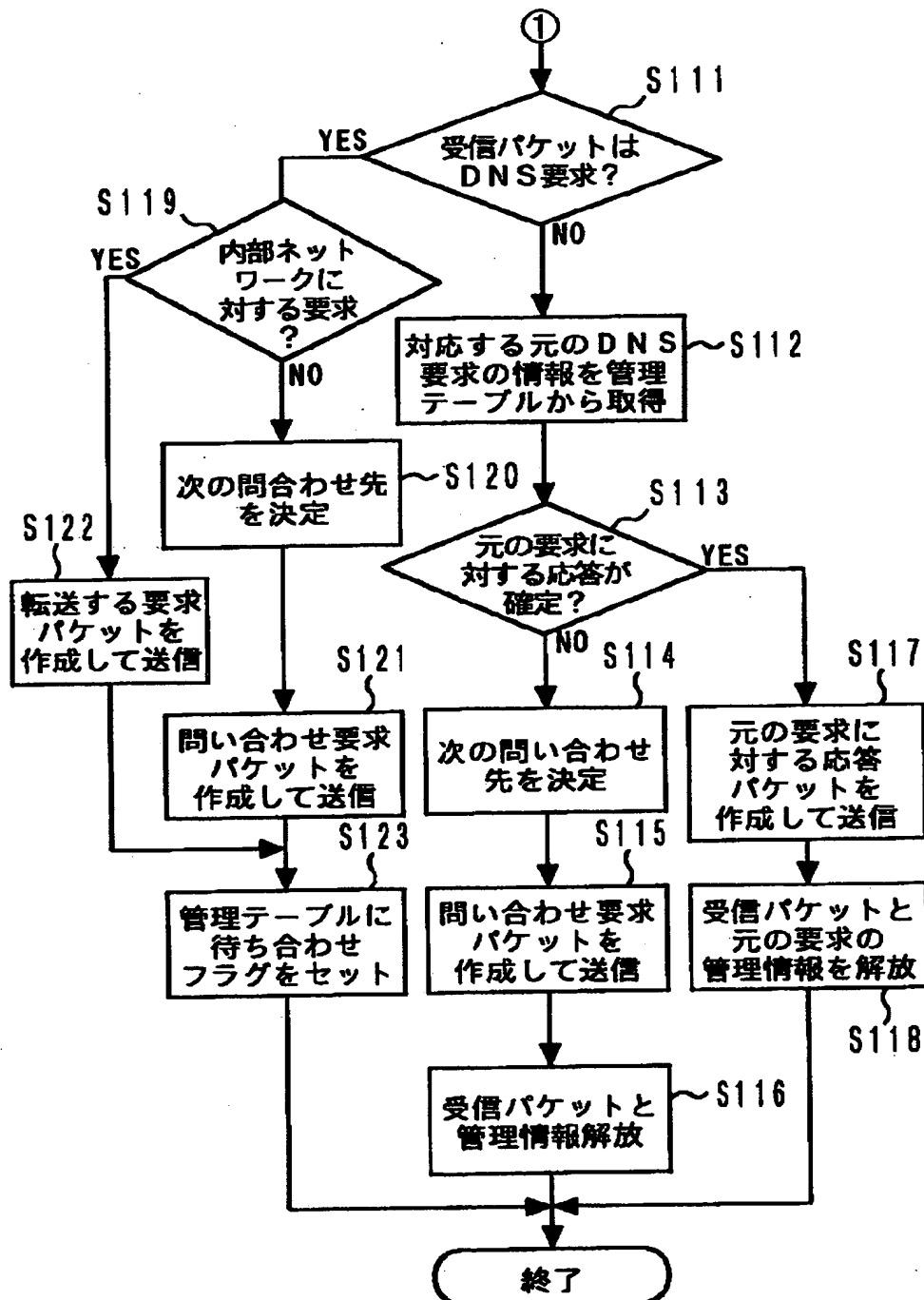
【図4】



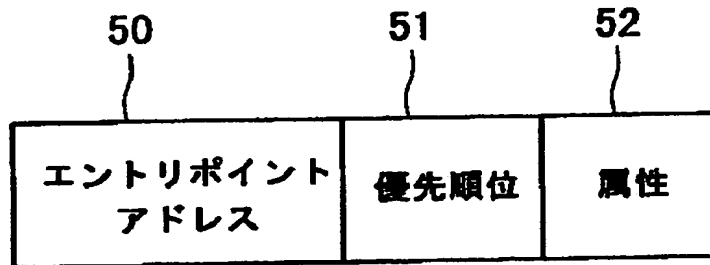
【図 5】



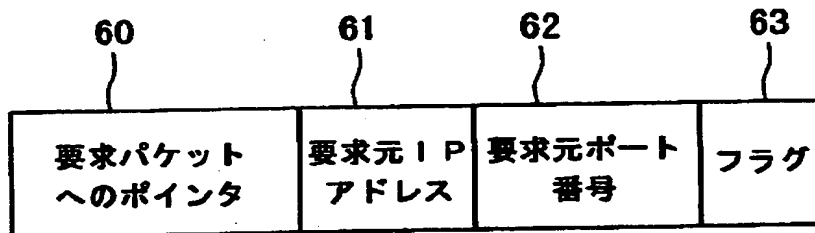
【図 6】



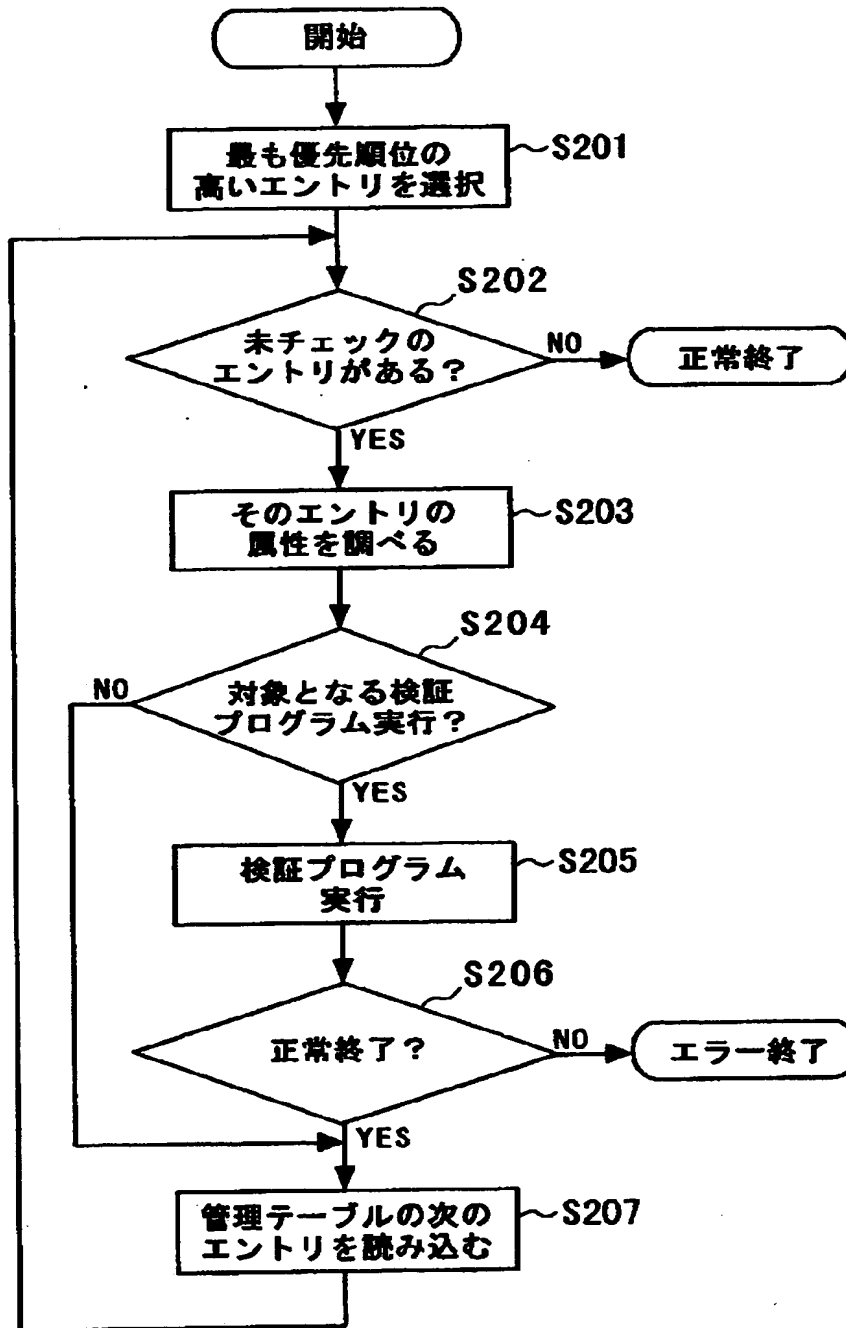
【図 7】



【図 8】



【図9】



【書類名】 要約書

【要約】

【課題】

組織外の者が組織のネットワーク構成情報を利用して組織のネットワークに侵入を行うことを防ぎ、異常な形式のパケットを受信することでDNSサーバの動作が異常になることを未然に防ぐDNSサーバフィルタの提供。

【解決手段】

DNSプロトコルにおける端末及びDNSサーバからの問い合わせ、及びDNSサーバからの応答パケットを受信するパケット受信部と、問い合わせ要求を管理するためのセッション管理テーブルを備え、問い合わせ及び応答パケットを管理し全体の制御を行うセッション管理部と、問い合わせ及び応答パケットが異常であるか否かを検査するパケット検証部と、DNSサーバへの問い合わせパケットを生成する要求生成部と、問い合わせパケットの送信元に返す応答パケットを生成する応答生成部と、問い合わせ及び応答パケットを送信するパケット送信部と、を備え、受信したDNSパケットをDNSサーバに渡す前に、内容に異常があるか否かを検査し、異常を検出した際にエラー応答パケット生成して要求元に返す。

【選択図】

図 1

出 願 人 履 歴 情 報

識別番号 [000004237]

1. 変更年月日	1990年 8月29日
[変更理由]	新規登録
住 所	東京都港区芝五丁目7番1号
氏 名	日本電気株式会社